REMARKS

This is in response to the Office Action mailed February 14, 2003. Applicant has filed herewith a Request for Continued Examination and seeks further review of pending Claims 1-10 and 13-17.

Claims 1-10 and 13-15

By the previous Action, the Examiner rejected Claims 1-10 and 13-15 as being anticipated by or unpatentable over U.S. Patent No. 5,643,086 to Alcorn. In response to Applicant's previous arguments, the Examiner asserts that Alcorn teaches an encryption/decryption authentication procedure that is used on all casino game software, both programs and fixed data sets, which the Examiner interprets as "operating code/operating data" as claimed in Applicant's claims.

Applicant agrees with the Examiner's assertion that Alcorn discloses applying an authentication procedure to all casino game software, including programs and fixed data sets. However, Alcorn does not teach or suggest an authentication procedure in which the programs and fixed data sets are encrypted. Instead, Alcorn teaches generating a bit string from each program or data set. This bit string comprises a signature which is used to verify or authenticate the program or data set. To protect this important signature, the signature is encrypted. Each signature is stored along with its corresponding unencrypted program or data set. Authentication is performed by generating a second bit string and comparing that bit string to the decrypted bit string or signature. See Alcorn Col.2, lines 44-65.

Thus, in accordance with Alcorn, an encrypted signature is provided along with a non-encrypted data set. As the Examiner indicates, Alcorn teaches authenticating each program or data set. In Alcorn, authentication comprises checking the signature accompanying the non-encrypted data set.

Applicant asserts that this is a fundamental difference between Applicant's invention and Alcorn. In accordance with Applicant's invention, the operating code or operating data is itself encrypted and is thus protected. In Alcorn, only a signature generated via a hash function run upon such data is encrypted. Alcorn does not teach encrypting the actual program code or operating code/ data.

Further, Applicant asserts that this difference is not obvious in view of Alcorn. Alcorn teaches a method of authenticating data using a signature generated by a hash function. Applicant's invention is directed to a method of protecting information by encrypting the data itself. Applicant's invention and Alcorn's method are thus done for different purposes, and they yield different results.

Applicant asserts that independent Claim 1 is believed to be allowable over the prior art, including Alcorn, for at least the reason that the claim recites a method of decrypting encrypted operating code (and not a signature comprising a bit string calculated from the code). Alcorn does not teach a method of decrypting and using code, but only generating authentication data from a data set and comparing that authentication data to a decrypted bit string. Applicant further notes that Claim 1 recites the step of utilizing the decrypted code to control a gaming device. In Alcorn, even if one attempts to construe the hash-generated signature as code, that signature does not comprise control code used to control the operation of the gaming device.

Independent Claim 5 is similarly believed to be allowable over the prior art, including Alcorn, for at least the reason that the claim recites a method in which actual operating data is encrypted (and not a signature comprising a bit string generated from the code, as in Alcorn). Claim 5 also recites the step of utilizing the data in the operation of the gaming device to present a game.

Independent Claim 10 is believed to be allowable over the prior art, including Alcorn, for at least the reason that it recites a gaming device including a memory for storing encrypted operating data, a separate secure access module for storing a private decryption key, and a separate programmable memory for storing decrypted data for use. Applicant asserts that Alcorn does not teach a gaming device having all of these elements configured to decrypt and utilize operating data in the operation of the gaming device. Further, Applicant asserts that Alcorn does not disclose use of a SAM. As disclosed in the specification of the present application, a SAM comprises a computing module capable of decrypting encrypted data using an accompanying private key. See ¶ [0031]. Alcorn teaches only storing a key in a ROM. The ROM is simply a memory, and does not comprise a SAM which is independently capable of decrypting data.

Claims 16-17

The Examiner indicated the rejection of Claims 16-17 under 35 U.S.C. § 103 as being unpatentable over Alcorn in view of Wright (USPN 6,052,466) or Eliott (USPN 6,468,150). The Examiner asserts that Wright and Eliott teach the use of multiple private keys to encrypt different parts of operating data in a computer system.

Applicant asserts that neither Wright nor Eliott teaches or suggests the aspect of the invention as claimed comprising encrypting first and second portions of operating data with first and second keys and providing only one of those keys to a gaming device, thus permitting only the portion of the code encrypted with the provided key to be decrypted.

Eliott actually does not teach encrypting different portions of code with different keys. As indicated in the Abstract, Eliott does disclose storing separate portions of a video game in different partitions. As provided at Col. 34, line 30 to Col. 35, line 16, in accordance with Eliott a hard disk may be divided into three partitions. Game code may be stored in one partition. This game code may be encrypted. Another of the private partions may be used to store game data in read-only format, and yet another portion may be used to store player scores or the like. The information in these latter partitions is not encrypted. Eliott thus does disclose encrypting certain information using a key format. Eliott, however, does not disclose encrypting different portions of code with different keys, as Eliott teaches that only the game code portion of the code need be encrypted at all. Eliott also does not teach encrypting two portions of game code with different keys and providing only a single of the keys, thus permitting only a portion of the code to be decrypted, as claimed.

Wright teaches a system of encrypting individual packets of data in a communication network. As disclosed in Wright's Summary, each packet may be encrypted by a cipher stream generated from a different secondary key. Wright thus does not teach or suggest the invention as claimed. First, Wright teaches encrypting each data element with a single key. In accordance with the invention as claimed, a first portion of code is encrypted using a first key, and a second portion

with a second key. Wright does not teach or suggest dividing data packets and encrypting those portions with separate keys.

Further, in Wright each and every secondary key must be provided in order to decipher all of the packets in order to assemble the communication stream. In accordance with the invention as claimed, only one key is provided, thus enabling only a portion of the data which was encrypted with the corresponding key to be decrypted. The remaining code encrypted with the other key or keys remains encrypted and unusable.

Applicant asserts that for at least these reasons alone, Claims 16 and 17 are allowable over the prior art, including Alcorn, Wright and Eliott.

Summary

Applicant asserts that Claims 1-10 and 13-17 are in a condition for allowance and respectfully requests a notice as to the same. If any matters remain outstanding, the Examiner is invited to contact the undersigned by telephone.

Respectfully submitted,

Dated: May 13, 2003

By: _____

R. Scott Weide
Registration No. 37,755
Weide & Miller, Ltd.
7251 W. Lake Mead Blvd., Suite 530
Las Vegas, NV 89128
(702)-382-4804 (Pacific time)